International Journal of Digital Crime and Forensics
Volume 12 • Issue 3 • July-September 2020

Mobile Cloud Forensic Readiness Process Model for Cloud-Based Mobile Applications

Puneet Sharma, Amity University, India

Deepak Arora, Amity University, India

T. Sakthivel, Firstsoft Technologies Pvt. Ltd., India

ABSTRACT

Nowadays, mobile cloud applications have attracted millions of smartphone users due to the proliferation of cyber technologies and a wide range of applications. Mobile cloud forensic investigation methodologies need tremendous growth due to the increasing crime incidents. The forensic readiness model plays a significant role in the forensic investigation framework by ensuring the ease of investigation to the forensic investigator. The existing forensic readiness supports either the mobile device or cloud environment, which lacks to prepare the information for the investigation. This article presents a mobile cloud forensic readiness process model to identify the factors and prepare the information that effectively supports forensic investigations. The proposed model involves requirements for the mobile cloud forensics from multiple perspectives with the aim of developing the forensic-ready system. As a result, the proposed forensic readiness model enables the mobile cloud forensic to improve the accuracy of investigation as well as reduces the investigation time significantly.

KEYWORDS

Cloud-Based Mobile Application Infrastructure Readiness, Forensic Readiness, Mobile Cloud Forensic Readiness, Mobile Cloud Forensics, Time Synchronization

1. INTRODUCTION

The increased usage of mobile computing devices plays a significant role in planning daily routines, schedules, and activities over the Internet and facilitates ease of communication. In particular, smartphones have been widely utilized as a powerful computing device like a desktop or laptop computer (Muhammad & Soomro, 2013). However, the applications in Smartphones require high processing power, which is further addressed by cloud computing that offers the computing ability available to mobile users. The rapid development of Information and Communication Technology (ICT) have enabled the organizations to design, build, and run their operations in the Cloud environment. Mobile cloud computing (Shafique, Ahmad, & Rafique, 2011) provides the opportunity for mobile users to meet their increasing functional demands. However, the cloud-based mobile applications have opened a new horizon for adversaries to launch cyber-attacks and security breaches in which the adversaries misuse the advantage of the cloud services. The malicious activities have been launched over the Internet-based bullying such as in social networking, email, and instant

DOI: 10.4018/IJDCF.2020070105

messaging applications. The digital forensics techniques often face numerous challenges owing to the dramatic increase of cybercrime landscape with the significant knowledge of cyber technology (Raymond, 2011).

To deal with the cybercrime activities in the cloud-based mobile applications, integrating mobile forensics and cloud forensics has become a significant research area (Ben, Do, & Choo, 2015). Mobile forensics and cloud forensics are part of digital forensic science, which is the process of investigating the mobile computing and cloud computing platforms with the help of scientific approaches (Muhammad, Kechadi, & Le-Khac, 2015). However, the forensic process begins only after the incident takes place without forensic readiness that significantly impacts forensic process and analysis. Indiscriminately investigating the data with the inappropriate procedure and process has led to the consumption of time and unacceptable evidence presentation. In the mobile cloud forensic framework, law enforcement system requires the committed time of a crime or identified and reported time of the crime. Hence, there is a need for developing a forensic readiness model in the forensic investigation framework to avert the inaccurate evidence acquisition and extended investigation period (Antonio & Labuschagne, 2012). Digital forensic readiness (Ausra, 2017) is one of the abilities of an organization in minimizing the investigation cost and maximizing the applicability of the evidence. Several researchers have presented the forensic readiness efforts in various perspectives include implementing the policies and processes of the organizations, appropriately training the employees, and aligning the systems based on the forensics objectives (Kamil & Venter, 2013). Recently, the researchers have focused on introducing the forensic readiness strategy such as forensic-by-design (Rahman, Hidayah, Glisson, Yang, & Choo, 2016). Nonetheless, the existing researchers fail to develop the forensic readiness model for the mobile cloud forensic investigation framework. Hence, it is necessary to develop the mobile cloud forensic readiness model with the target of improving the investigation accuracy and reducing the investigation cost on the cloud-based mobile applications.

2. RELATED WORKS

Most of the researchers provide valuable contributions to the development of the mobile forensic readiness model and the cloud forensic readiness model separately. This section reviews several prominent efforts about mobile device forensic readiness and cloud forensic readiness.

2.1. Mobile Forensic Readiness Approaches

Mobile forensic readiness model targets to ease the forensic investigation in the mobile device with the reduced time complexity and cost. Several research works have highlighted the necessity of new digital forensic tools and techniques to investigate a crime event, involving live investigations. A literature work (Soltan, Weber-Jahnke, & Traore, 2011) has reviewed the existing processes involved in the digital proactive and reactive forensic investigation process. A digital forensics framework (Grobler, Louwrens, & Solms, 2010) enforces the organizations to perform a proactive forensic investigation. In order to achieve forensic readiness in an organization, several systematic and conceptual frameworks (Mohamed, Maynard, Ahmad, & Lonie, 2014; Mohamed, Ahmad, Maynard, & Lonie, 2015) have been introduced by exploring the factors that support forensic readiness. A harmonized Digital Forensic Investigation Readiness Process (DFIRP) model (Aleksandar & Venter, 2013) provides the guidelines for the investigation process through readiness processes such as planning, implementation, and assessment. This digital forensic readiness model has to be adapted to various organizations, which ensures an effective and efficient forensic investigation with the provision of admissible digital evidence to the court.

Smartphone forensic investigation process model (SPFIPM) (Archit, Tyagi, & Agarwal, 2012) incorporates the forensic preparation phase to guide the smartphone investigation effectively. It explores the fourteen-stages of smartphone forensics process model with the target of finding the potential evidence. A forensic analysis of Symbian smartphones approach (Zian, Jiang, Shu, Yin,

& Liu, 2009) addresses the difficulties involved in applying the traditional investigation method on Symbian smartphones by integrating the preparation and version identification process as a prerequisite task of the smartphone forensics. The mobile forensic readiness model (Serra & Venter, 2011) addresses the cyber-bullying problem by delivering a proactive solution. It enables the risk determination based on the risk profiling analysis of a user, which assists in identifying a threat using the neural net system dynamically. A proactive investigation scheme (Alexios, Meletiadis, Tsoumas, Mitrou, & Gritzalis, 2012) examines the connection channels that are used for transferring the evidence during a forensic investigation, which includes the prevention mechanism to protect smartphone users from misuse by malicious entities. With the target of minimizing cyber-bullying, a mobile forensic readiness model (Kebande, Karie, & Omeleze, 2016) enhances the awareness about the cyber-bullying issues and creates the parental guidance information regarding cyber-bullying.

2.2. Cloud Forensic Readiness Approaches

Most of the research works have attempted to present the digital forensic readiness model in the cloud environment to improve the cloud forensic investigation. A Cloud forensic readiness system (CFRS) (Kebande & Venter, 2014) is based on a Botnet as a service, which transforms the botnets from illegal to legal monitoring as well as information capturing applications to provide the admissible digital evidence to the court. In the cloud environment, cloud providers utilize the digital forensic readiness model to manage the data that are essential for forensic investigation. However, this digital forensic readiness model fails to examine the readiness of the data for further forensic analysis in a cloud environment (George, Fogwill, Venter, & Ngobeni, 2013). By considering a remote and central logging facility in a cloud environment, the digital forensic readiness model in Trenwith and Venter (2013) accelerates the data collection in the forensic investigation. A conceptual framework (Percy & Leonard, 2014) determines the readiness state of the Cloud service providers (CSPs), which incorporates a process tool and also, enables the organizations to achieve accurate decision making and suitable CSP selection. Later, a conceptual forensic readiness framework (Nour, Ithnin, & Miakil, 2014) supports the cloud IaaS consumers to acquire the required evidence without depending on the CSPs.

This conceptual framework comprises nine components, including the forensic readiness of elements of technical, legal, and organization level. The CFRS (Kebande & Venter, 2016) employs the non-malicious botnet (NMB) solution to prepare the requirements for the cloud to be forensically ready based on the technical, legal, and operational perspectives. It presents the requirements for the digital forensic readiness in a cloud environment involves that the guidelines of information technology, incident investigation principles, security techniques, and incident investigation processes. In order to prepare the requirements for cloud forensic investigation, the research work in Moses, Venter, Eloff, and Eloff (2014) analyzes the implications of the forensic investigations in the cloud environment and presents three-tier digital forensic readiness model with the fundamental requirements for the cloud forensic investigation, which significantly minimizes the business disruption with the minimal amount of time and cost consumption during evidence acquisition. A novel digital forensic readiness model (Kebande & Venter, 2017) employs a modified obfuscated NMB that operates as a distributed forensic Agent-Based Solution (ABS) in a cloud environment. With the consideration of SLAs, it performs the forensic logging for forensic readiness without interfering with the operations and functionalities of the cloud.

3. MOBILE CLOUD FORENSIC READINESS MODEL

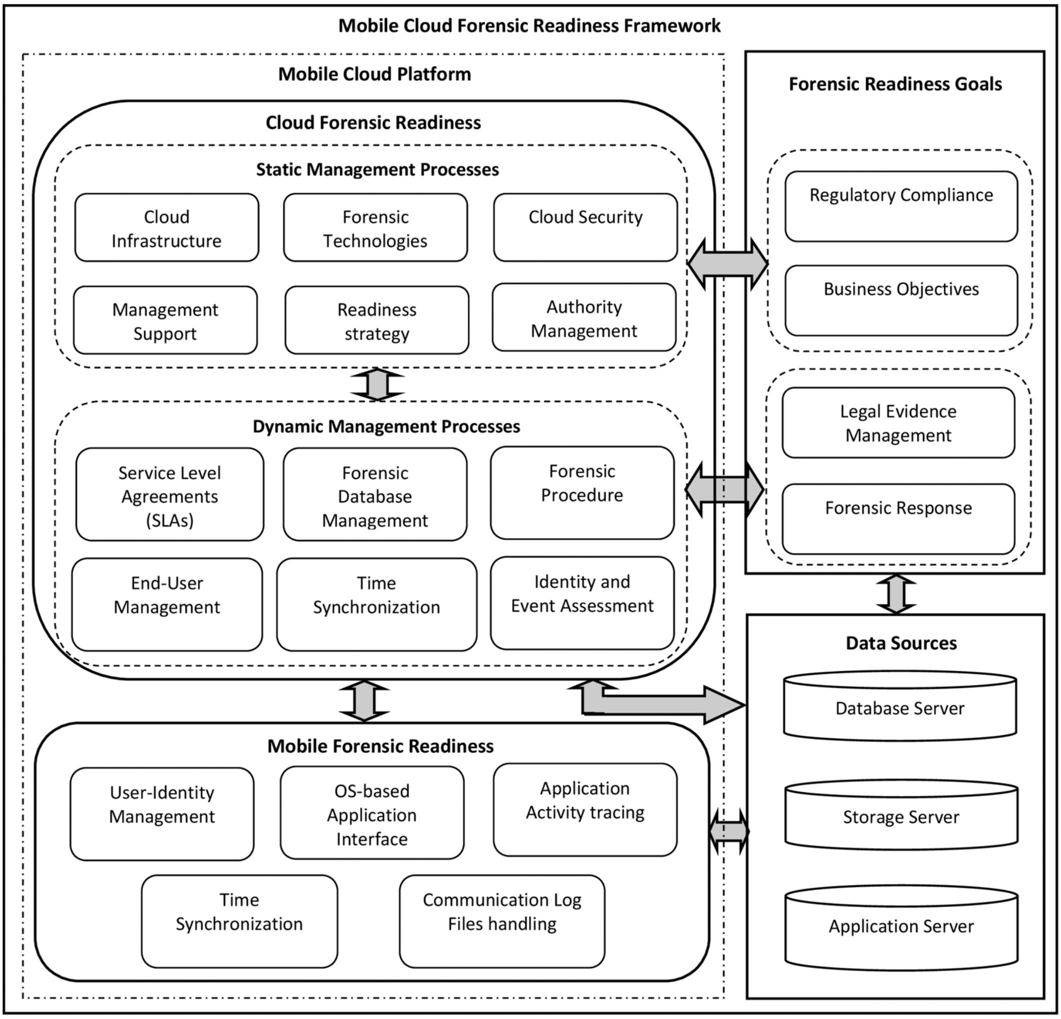
In the digital forensics field, the primary objective of the forensic readiness is to maximize the potential of an organization to create the feasibility of performing forensic investigation and to access the digital evidence within the minimum cost of an investigation. Fundamentally, the main objective of forensic readiness is to ensure the pertinence and completeness of the evidence for the forensic investigation._Digital forensic readiness process involves the implementation of an information system that can record the potential evidence, evidence encryption, and evidence storage to facilitate the crime scene investigation. In essence, the forensic readiness process includes several steps such as retaining information, planning the incident response, training the forensic tool to handle the investigation, accelerating the investigation, preventing anonymous activities, and protecting the evidence. As a result, the forensic readiness phase provides various benefits to the investigator, including i) cost minimization of the investigation, ii) easier to understand the dynamics of a cyber incident, and iii) post-incident activities optimization in terms of effort, time, and cost. In organizations, forensic readiness considers seven factors such as technical stakeholders, non-technical stakeholders, monitoring, architecture, technology, training, and policy to apply the forensic strategy (Mohamed, Maynard, Ahmad, & Lonie, 2014). In mobile cloud forensic framework, both the mobile and cloud necessitates the forensic readiness process before initiating the forensic investigation to access the evidential artifacts regarding the mobile cloud application execution. To acquire credible evidence from both the mobile and cloud, forensic readiness is crucial that maximizes the ability of an environment and minimizes the cost of the investigation.

Several existing forensic readiness research works have introduced different proactive and reactive solutions for the digital forensics (Mohamed, Maynard, Ahmad, & Lonie, 2014, 2015), mobile forensics (Mohamed, Maynard, Ahmad, & Lonie, 2015; Serra & Venter, 2011), and cloud forensics (Trenwith & Venter, 2013; Makutsoane & Leonard, 2014). Despite the certainty, the forensic investigation is a time-consuming and costly process. Hence, it is worth to apply forensic readiness procedure to ease the collection of forensic evidence for reducing the investigation cost and time. Thus, the proposed approach systematically enhances the existing forensic readiness procedures that are essential for the mobile cloud forensic investigation. It adaptively integrates digital forensic readiness, mobile forensic readiness, and cloud forensic readiness models to aid the forensic investigation in the mobile cloud environment.

To mitigate the complexities during the investigation and improve the investigation accuracy, incorporating the forensic readiness component is essential in the forensic framework. In the context of mobile cloud forensics, the investigator requires forensic readiness as the pre-investigation process in both the mobile and cloud environments. Forensic readiness phase includes the process of identity management, event management, encryption management, and interoperability. In the forensic readiness phase, the first two processes are necessary procedures for both the mobile and cloud environment, whereas, the latter two processes are vital only in a cloud environment. Identity management is the ability to manage the identity of individual users and their authorization, authentication, roles, and permissions to access the data on the mobile device as well as the cloud environment. Event management is the process of conceptually constructing the event based on the requirement under crime scene investigation on the device and cloud. It involves event construction, event freezing, event traceability, time sequence, and event reconstruction. Encryption management is the process of searching, acquiring, and accessing the encrypted forensic data in the distributed cloud environment while concerning the multi-tenancy and multi-jurisdiction issues. Interoperability refers to the ability to ensure forensic readiness in the inter-cloud environment.

Figure 1 shows the block diagram of the mobile cloud forensic readiness model. Forensic readiness is the process of proactive digital forensics, which can determine the required evidence type and incident time in advance. In the context of the mobile cloud environment, the primary objective of the forensic readiness is establishing the lineage between the application activities in the mobile device and the cloud to improve the feasibility of evidence collection and minimize the cost of the forensic investigation. Instead of determining the event logs in the mobile device and the cloud during mobile forensics and cloud forensics respectively, the mobile cloud forensic readiness additionally includes the process of identity and event assessment. The proposed mobile cloud forensic framework incorporates the forensic readiness phase for the smartphone and remote Cloud as a part of the contribution with time synchronization along with the identity and event assessment to enhance the traditional mobile cloud forensic process. With the target of ensuring both the investigation accuracy and time efficiency

Figure 1. Mobile cloud forensic readiness framework



in the investigation, the proposed framework enforces the reactive investigation by proactive analysis in the mobile cloud environment. The proposed forensic framework incorporates several essential steps in the forensic readiness phase for the mobile cloud environment that involves incident recognition, authorization, infrastructure readiness, procedure readiness, and time synchronization. According to Figure 1, the goals of forensic readiness mainly include four capabilities such as regulatory compliance, business objectives, legal evidence management, and forensic response in a mobile cloud environment. The framework of forensic readiness is based on the 'objectives or goals' terminology. The forensic readiness model additionally focuses on the business objectives and forensic response instead of only considering the legal evidence management. The forensic readiness framework assists organizations in responding to incidents appropriately:

- **Legal Evidence Management:** It is the ability of an organization to provide digital evidence that is to be used for preceding the legal investigation activities such as legal defense, commercial disputes, e-discovery orders, and prosecution;

- **Regulatory Compliance:** It is the ability of an organization to reveal the adherence to laws and regulations in the state of utilizing evidence in the forensic readiness perspective. In order to avoid non-compliance and to produce legally sound evidence, regulatory compliance has been used as the most significant objective of organizations in the forensic field. In essence, the organizations can respond to incidents, to create their data discoverability, ensure the incidents that are reported, and to retain the financial records;
- **Business Objectives:** Business objectives of the organization include maintaining the reputation, reducing the forensic investigation cost, improving the security strategy concerning the investigation results, mitigating the disruption on business during the investigation, estimating the impact of incidents, enhancing the interaction interface with law enforcement, and incorporating data recovery. By adopting the forensic readiness, business objectives are indirectly related to the forensic investigation;
- **The Forensic Response:** It is the process of initiating the forensic investigation by responding to incidents at reducible investigation cost. It is capable of allowing the organizations to perform a digital investigation and provide reliable and relevant digital evidence within the minimum cost promptly.

With the aforementioned forensic readiness objectives or goals, the forensic readiness model adapts its procedures to the mobile cloud platform. In the mobile cloud forensic readiness framework, mobile forensic readiness necessitates several preliminary steps that are to be performed before initiating the forensic investigation.

Mobile forensic readiness module incorporates the processes such as user-identity management, Operating System (OS)-based application interface, application activity tracing, time synchronization, and communication log files handling:

- **Identity Management:** It is essential to ensure transaction validity between a particular user and the service provider in a seamless manner, which minimizes the management overhead and protects services, resources, and user data. In the context of forensics, identity management ensures the cost-effective as well as a scalable investigation from the perspective of users and the service providers;
- **The OS-Based Application Interface:** It is a crucial task for the smartphone forensics due to the diversity of OSs and the applications exploited by smartphones. In order to extract the evidence, especially, the activities performed by a specific application from the suspected device, analyzing the application interface concerning the type of OS and the application are a prerequisite to adapt the forensic investigation methodology;
- **Application Activity:** It tracing paves the way for the investigators to extract and examine the remnants of the event in a forensically sound manner;
- **Time Synchronization on the Device:** It becomes a crucial process in both the smartphone and the cloud to leverage the accurate evidence collection without losing the significant evidence since there is the open space for manually changing the time of the mobile device by anyone;
- **Communication Log Files Handling:** It is the process of monitoring the communication logs performed through smartphones and enabling the storage facility for the corresponding application activities over the Internet, which examines the substantial amount of evidence throughout the investigation.

Cloud forensic readiness module divides its forensic readiness process into static management factors and dynamic management factors. Static management processes include cloud security, cloud infrastructure, forensic technology, management support, readiness strategy, and authority management:

- **Cloud Security:** The security programs are necessary for the digital forensics field, which helps to detect the incident by monitoring the system promptly with the assistance of various technologies such as anti-spyware technology, anti-virus, and intrusion detection system (IDS);
- **Cloud Infrastructure:** To support the digital forensic investigation in the cloud with the subsequence of the mobile forensics, preparing the underlying infrastructure is necessary. The cloud infrastructure preparation involves the system, networking, and laboratory preparation;
- **Forensic Technology:** To perform a digital investigation, applying forensic technology is vital for both the mobile and cloud platform, especially, the cloud environment essentially requires the forensic technology before initiating the investigation to handle the sequence of the mobile forensics activity. Forensic technology includes specialized forensic tools or software to accurately collect the evidence, which aids to provide the admissible evidence reliably;
- **Management Support:** In the cloud environment, management support involves authorization, funding, decision making, and so on. To facilitate the forensic investigation, preparing the support structure of an organization at the top management level is crucial;
- **Readiness Strategy:** Developing readiness strategy based on the legislation of the international standards has become a significant component in the cloud forensics fields. The readiness strategy pertains to the working procedure of the forensic readiness in the cloud, involves the identification of the possible source of evidence and hypothetical scenarios, and budget planning;
- **Authority Management:** Authority management facilitates the investigator and the cloud service provider to deal with the incident management in a large-scale environment. It manages user identification based on the user profile information. The authorization capability provides the access control policy to the cloud resources.

Moreover, in the cloud forensic readiness model, the dynamic management processes involve SLAs analysis, forensic database management, forensic procedure, time synchronization, end-user management, and identity and event assessment. Identity and event assessment is processed similarly to the process involved in the mobile forensics readiness model:

- **Service-Level Agreements:** Service level agreement (SLA) refers to the contract between the end-user and the cloud service provider, involving the services offered by the provider such as forensic investigation. It specifies the responsibilities of the user and CSP, which performs the cloud data investigation in a forensically sound manner;
- **Forensic Database Management:** In the cloud environment, managing the forensic databases is essential to ascertain the admissibility of the evidence and also, to reveal the anti-forensics method based on evidence missing during the investigation. Hence, enabling the forensic database is non-trivial in the readiness process to automatically store the records of names of files and folders with time which are involved in the forensic investigation;
- **Forensic Procedure:** To guide the dynamic cloud forensic investigation, the cloud forensic readiness phase focuses on modeling the forensic procedures, instructions, and guidelines with respect to the crime event. In the mobile cloud environment, the forensic procedure involves both proactive and reactive procedures based on the subsequence of mobile forensics evidence;
- **End-User Management:** With the impact of mobile forensics, the mobile cloud forensic readiness model needs to manage the process, and stored data belongs to the suspected end-user in the cloud. The cloud forensic readiness model associated with the end-user management process plays a key role in reducing the investigation cost and complexity in a large-scale cloud environment;
- **Time Synchronization on the Cloud:** In the cloud forensics, time synchronization is a crucial factor due to the mobility and distributed resources in the cloud environment. In the distributed cloud environment, the VM migration necessitates the time synchronization among the suspected user data stored data centers. It is because the clock of OS varies from the datacenter to datacenter.

To reduce the complexity of the investigation, time synchronization is associated with the cloud forensics readiness model;

- **Identity and Event Assessment:** It is the interrelation process between the mobile device and the cloud, which is necessary for the mobile cloud forensic readiness before investigating the remote cloud for a particular crime event. The forensic readiness model needs to cross-validate the user identity and also, the crime event in the suspected mobile device with the cloud data.

3.1. Incident Recognition and Authorization

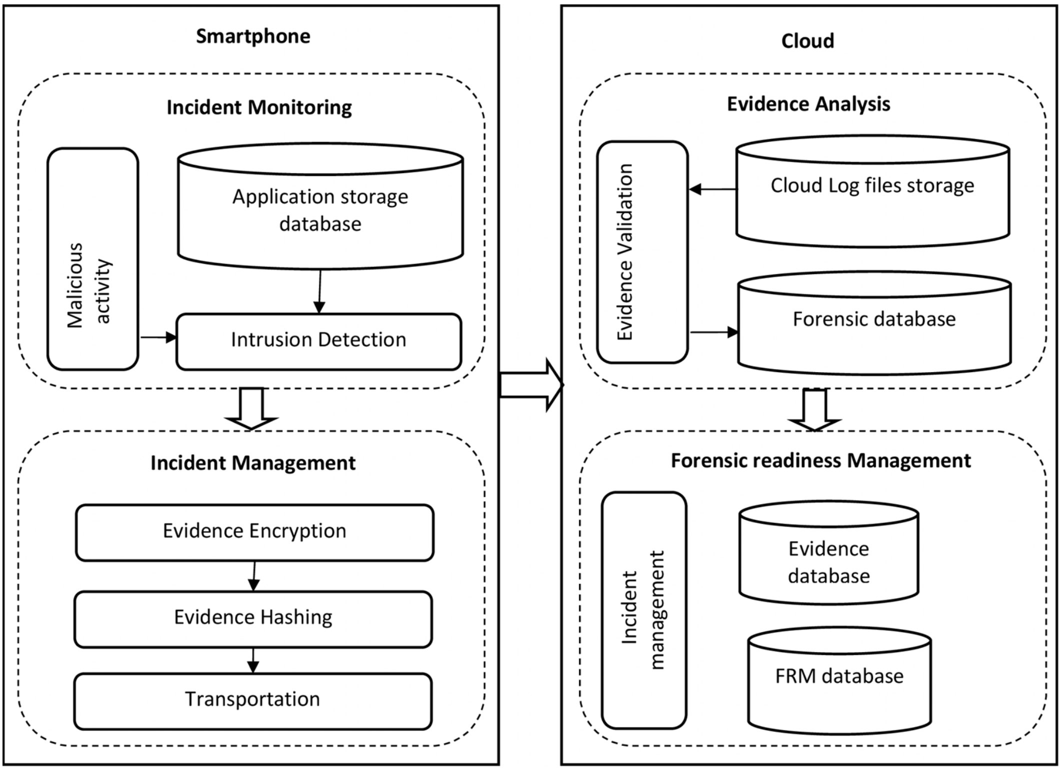
The proposed forensic readiness phase initially recognizes the nature of the crime scene and then, obtains the authorization for accessing the data. In order to generate the response to the incident, the forensic readiness phase needs to collect the log history or monitoring results in terms of integrity, reliability, completeness, and secure legal admissibility of evidences about the incidents. In the dynamic mobile cloud environment, it is necessary to perform the reactive forensic investigation by establishing forensic readiness instead of performing the restore-centered data protection-based incident responses and establishing an incident-counter strategy proactively. For the cloud-based smart environment, to conduct fast and efficient digital evidence collection and analysis, the forensic framework requires a preemptive analysis through digital forensic readiness. Thus, it averts the difficulty in collecting digital evidence after realizing that the incident has occurred.

While providing the incident response, the roles of the forensic readiness phase include several key prerequisites. These prerequisites involve i) determining the legislation and regulations which obligate the organization to retain the evidence, ii) identifying the sources of evidence within the concerned organization, and iii) finding the required procedures and technology to ensure the forensic readiness process. To conduct the cloud forensic investigation, performing proactive forensics is of crucial importance to assist the examination and analysis of digital evidence through forensic readiness process. By preparing the mobile device and the cloud for the forensic investigation, performing the event reconstruction process becomes a simple task that assists the pre-analysis of the characteristics of the potential incidents.

The proposed forensic readiness phase initially recognizes the nature of the crime scene and then, obtains the authorization for accessing the data (Figure 2). Later, it makes the infrastructure to be investigated for the corresponding crime scene and develops the investigation procedure according to the crime scene. Whereas, infrastructure readiness refers to preparing the device and cloud infrastructure for a specific application. For instance, WeChat application which is the primary source of potential evidence for the crime scene. Time synchronization is a vital factor in both the device and cloud to avoid inaccurate evidence collection and loss of potential evidence in the perspective of computational accuracy and time.

Figure 2 illustrates the steps involved in the incident response and authorization phase in the mobile cloud forensic readiness methodology. The essential processes that include incident monitoring and incident management in the Smartphone and evidence analysis and forensic readiness management in the cloud. The proposed methodology proactively monitors the incident in the mobile device by analyzing the application storage database with the help of an incident monitoring module. The forensic investigator needs to preserve the evidence in the smartphone from the device hacking throughout the investigation. Hence, the readiness component focuses on evidence hashing and encryption. In subsequence, the incident is to be validated in the cloud server and then, to be stored in the forensic database to ease the investigation. Finally, to provide the incident response and authorization, the proposed forensic readiness methodology dynamically manages the incident, evidence database, and forensic readiness management database. In the proposed mobile cloud forensic readiness models, the incident recognition and authorization for both the mobile and cloud environment utilize the enrichment of the previous incident response principles in the forensic investigation (Ahmed, Zulkipli, Atlam, Walters, & Wills, 2017). In the mobile cloud forensics, obtaining authorization process ensures the

Figure 2. Incident response in mobile cloud forensic readiness



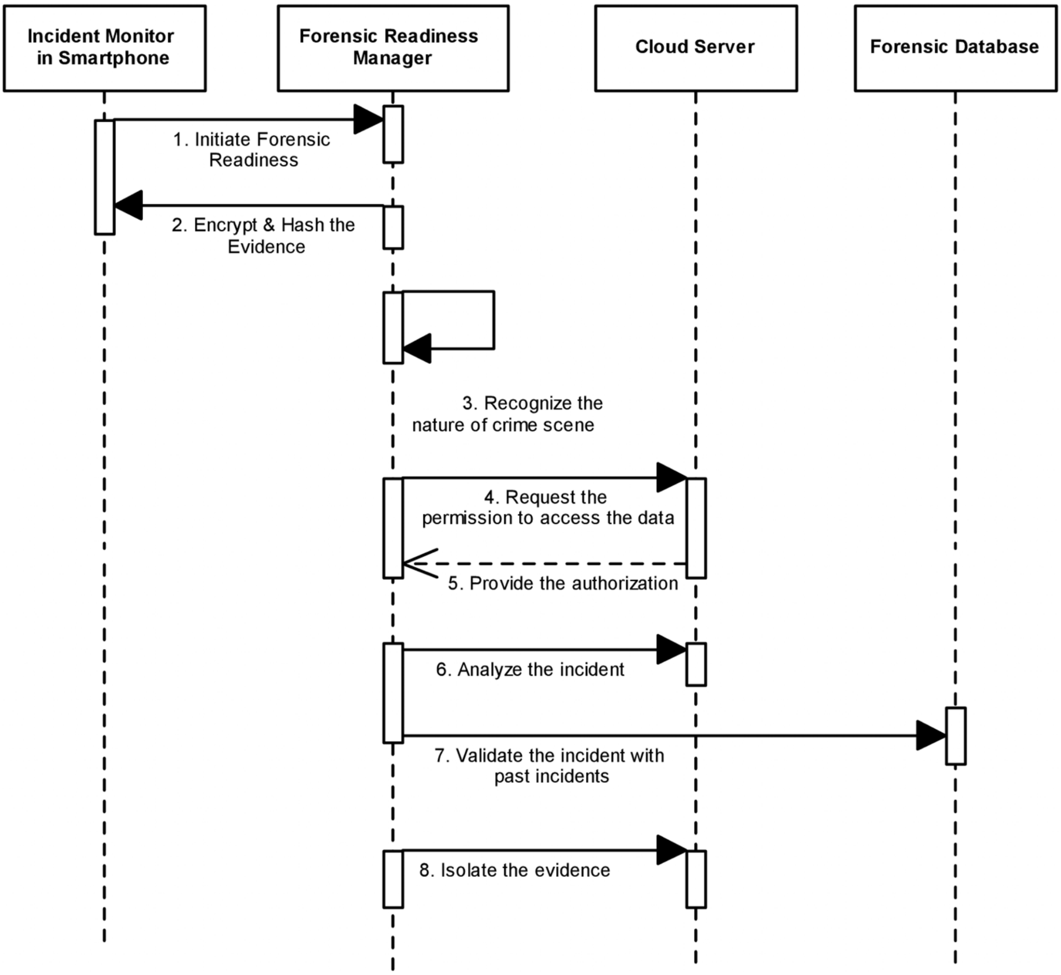
investigation process performed by the investigator under the proper authorization from authorities and legal provisions. Legal approval of the forensic investigation relies on the authorization process. In the context of mobile cloud forensics, authorization is based on different factors such as accountability, lines of authority, malicious entities, trust but verify. The sequential steps of the incident response in the mobile cloud forensic readiness phase are illustrated in Figure 3.

In order to preserve the evidence relevant to the incident during the investigation, the forensic readiness manager needs to isolate the evidence after the validation of the incident with the past incidents in the cloud server for ensuring secure investigation. It is because evidence isolation heavily relies on the characteristics and severity of the incident to avoid its negative consequences on the information of others in the cloud server.

3.2. Infrastructure Readiness

Infrastructure readiness is an on-going process which ensures that there is the availability of investigation-relevant data while occurring an incident. In the mobile device, infrastructure readiness involves the process of finding the source of evidence and the suspected device handling the investigation-relevant data. In the cloud environment, the CSP is responsible for the infrastructure readiness which is based on the SLA between the CSP and the cloud user. It is because there is a different level of logging and data retention requested by the cloud users when varying the operations between the CSPs and the user. During the forensic investigation, Law enforcement meets difficulty due to the consideration of the type and amount of available data; hence, infrastructure readiness is essential for the investigation process. In order to support the evidence collection, infrastructure preparation of the organization plays a significant role in the assistance of procedures, technologies, and policies. The forensic readiness model needs to prepare the infrastructure that is investigated

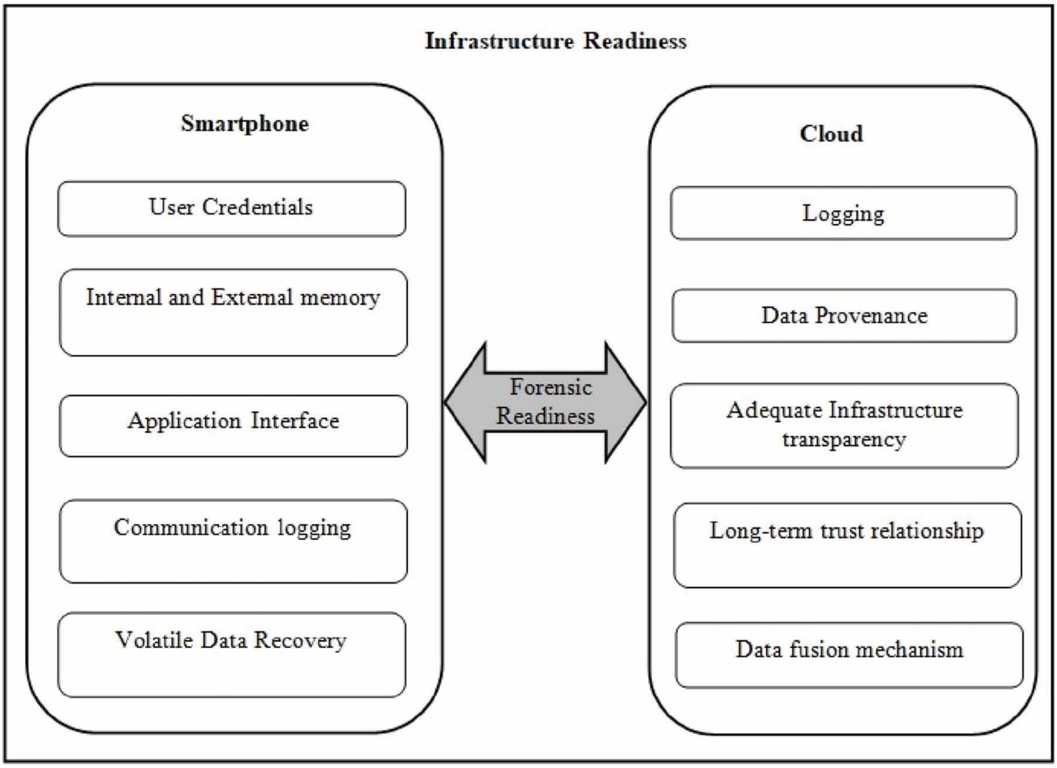
Figure 3. Sequence diagram for incident response in mobile cloud forensics


Incident Monitor in Smartphone
Forensic Readiness Manager
Cloud Server
Forensic Database
1. Initiate Forensic Readiness
2. Encrypt & Hash the Evidence
3. Recognize the nature of crime scene
4. Request the permission to access the data
5. Provide the authorization
6. Analyze the incident
7. Validate the incident with past incidents
8. Isolate the evidence

concerning the crime scene and to develop the crime scene-based investigation procedure. In the context of cloud forensics, infrastructure preparation involves the preparation of the system include physical and virtual resources and networking resources. The infrastructure readiness phase targets to ensure data integrity and stability throughout the investigation process, for example, securely storing evidence, hashing files, and dynamically maintaining the management database.

To perform the forensic investigation, the CSP needs to provide the service such as forensics as a service similar to the Software-as-a-Service (SaaS), Platform-as-a-Service (PaaS), and Infrastructure-as-a-Service (IaaS). In contrast to the restricted access in each of three cloud services, the forensic investigator requires open access for all the components involved in the cloud service layers. By associating the infrastructure readiness component, the forensic investigator automatically initiates the investigation through a single point of contact by the CSP. While preparing the infrastructure for the forensic investigation, the CSP ensures that there is the ability to obtain all the required information by the investigator without violating the SLA and privacy regulations. By providing the complete access control that is being ready before the forensic investigation, the investigation process becomes faster and more comfortable. In the infrastructure readiness, the complete access control of the cloud environment during investigation involves the application, data, OS, servers, and network access control. According to Figure 4, infrastructure readiness in the mobile cloud forensics includes both the mobile forensics readiness and cloud forensics readiness. The mobile forensics readiness phase needs to have the ability to obtain the user credentials, to access the internal and external memory, to prepare the required application interface, to access the communication logging, and to enable the volatile data recovery mechanism. The cloud forensic readiness phase needs to have the ability to perform the application logging, obtain the data provenance, enable adequate infrastructure transparency, provide long-term trust relationship, and apply the data fusion mechanism.

Figure 4. Infrastructure readiness in mobile cloud forensics



By considering the factors involved in the existing infrastructure readiness system (Aleksandar & Venter, 2013), the proposed approach develops the mobile cloud infrastructure readiness for the forensic investigation. In the mobile forensic readiness, user credentials involve username and password for the communication service, extracted from the user's Google account password sync service. In the smartphone, both the internal and external memory contains the evidential data about the activities performed by the applications. For example, WeChat app, Line app, and Viber app store their files and data in the internal memory of the device. Android applications generate their databases in the internal memory of the smartphone, which is inaccessible by the users. In contrast, the WeChat, Line, and Viber applications store the user profile pictures, sent and received images in the external memory that is Secure Digital (SD) card of the smartphone in which the stored information is accessible by the users. Application components are content providers that manage the accessed and shared data of the application. Application interface with the content providers is essential to access the application data. Communication logging is the process of accessing all the communication activities performed through the cloud-based mobile application. In the mobile forensic readiness, enabling the volatile data recovery mechanism is the essential process due to the increase of deleted information that contains the potential evidence regarding the criminal activity.

In the cloud forensic readiness, application logging is to be performed on the distributed servers since the cloud-based applications store its logs on the multiple files and servers. In the cloud environment, infrastructure logs provide a meaningful context for application logs. Data provenance plays a crucial role in the post-incident investigation, such as forensic analysis, which is to be monitored in the forensic readiness phase to provide the history of information includes people, activities, and entities involved in a related data processing. In order to initiate the investigation in the cloud, the CSP needs to provide the required infrastructure transparency to the forensic investigator of the crime scene. In the cloud forensic readiness phase, there is an essential need for maintaining a long-term trust relationship between the CSP and the forensic investigator throughout the investigation. Due to the distributed data storage in the cloud environment, the evidential data results from the multiple sources, hence, applying the data fusion mechanism is crucial to reconstruct the crime event to proceed the forensic investigation further effectively. Figure 5 shows the sequence diagram for infrastructure readiness in the mobile cloud forensics framework.

3.3. Procedure Readiness and Time Synchronization

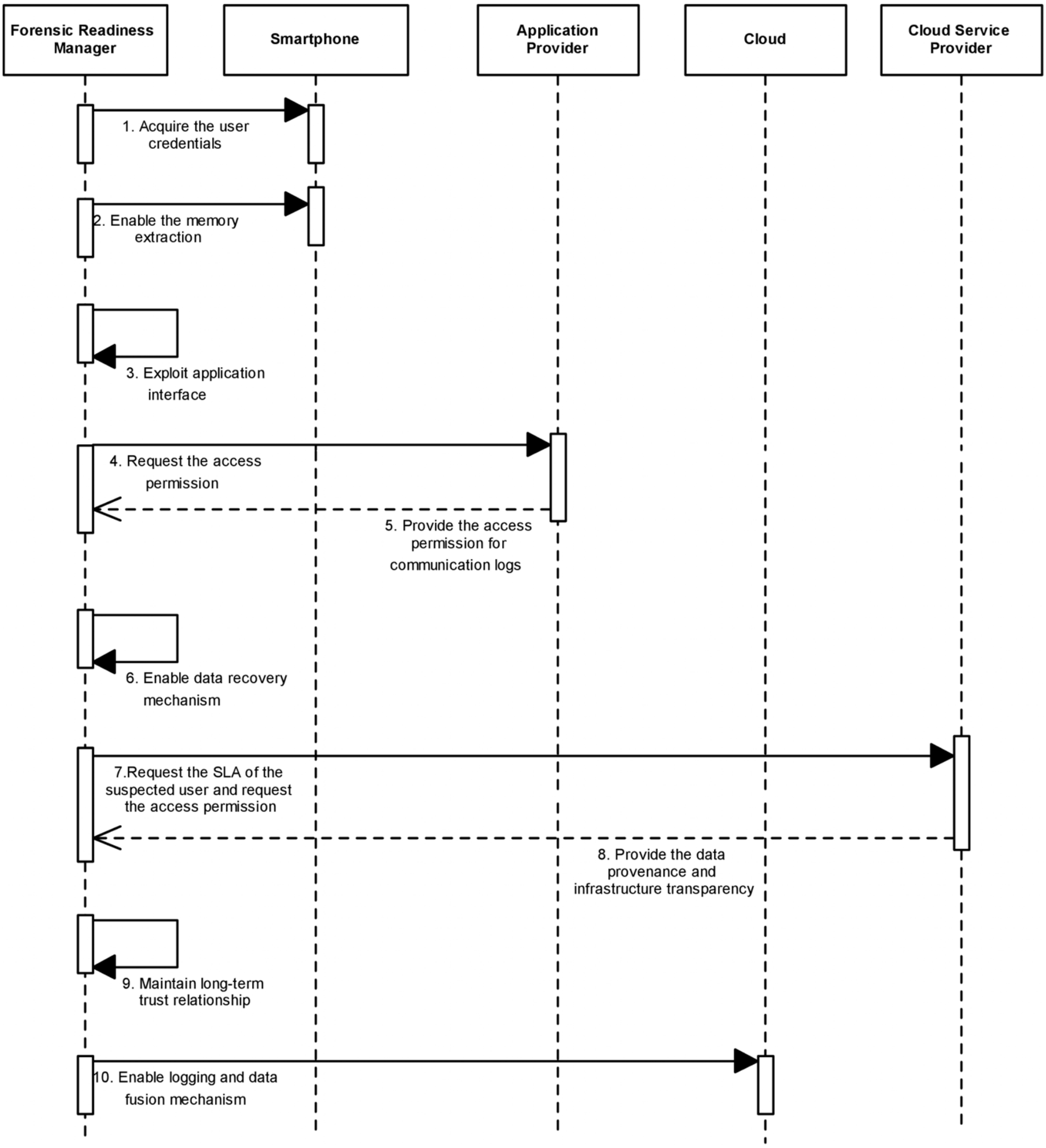
In the mobile cloud forensics, the forensic readiness phase especially, procedure readiness can prepare tools, techniques, and various procedures to facilitate the forensic investigation in both the mobile device and the cloud environment. Figure 6 shows the components involved in the mobile cloud forensic procedure readiness.

By analyzing the readiness factors in the existing systems (Aleksandar & Venter, 2013) and adopting the digital forensic procedure readiness model to the mobile and cloud forensic procedures with additional supportive factors, the proposed forensic readiness methodology ensures that a novel procedure readiness model effectively enforces the mobile cloud forensics. In the mobile forensic readiness, the procedure readiness involves that finding the mobile and application forensic tools, preparing the preservation procedure, developing user authorization monitoring mechanism, modeling deleted data recovery procedure for the OS and application type and formulating the incident response procedure in the mobile device. In the cloud forensic readiness model, the procedure readiness process includes many processes such as finding the appropriate cloud forensic tools and selecting preservation procedure with the consideration of data integrity to prevent the cloud evidence from either internal or external intruder or attacker. It is also modeling cloud authorization and monitoring mechanism, designing the deleted data recovery and the crime event reconstruction procedure concerning the artifacts type and location, and the developing incident response procedure in the cloud environment. Finally, the mobile cloud forensic strategy needs to be prepared before initiating the investigation process.

In modern Information Technology (IT) systems, virtualized environments often require timekeeping. It is essential to maintain timekeeping in two perspectives such as from the perspective of the CSP and the Client or user. The logs of the CSP and the other log files of the user log records are to be synchronized to precede the forensic investigation effectively. Timestamp information helps to identify the time of occurrence of a specific event. Due to the wrong time settings in the servers, clocks are drifted between a few seconds to hours, maintaining the time accuracy is essential in IT systems. The multiple aspects of managing, planning, securing, and debugging process require that the time of the event happened. Hence, time synchronization plays a vital role in the digital environment.

In the context of mobile cloud forensic readiness, time synchronization is a vital factor in both the device and cloud to avoid the inaccurate evidence collection and loss of potential evidence in the perspective of computational accuracy and time. To facilitate the forensic investigation, the CSP needs to synchronize the servers in the cloud environment to maintain the correct time of event logs. In addition to the CSP, the virtual machines also need to maintain the timekeeping. The timekeeping procedures often meet the difficulties in a distributed cloud environment especially, due to the distance

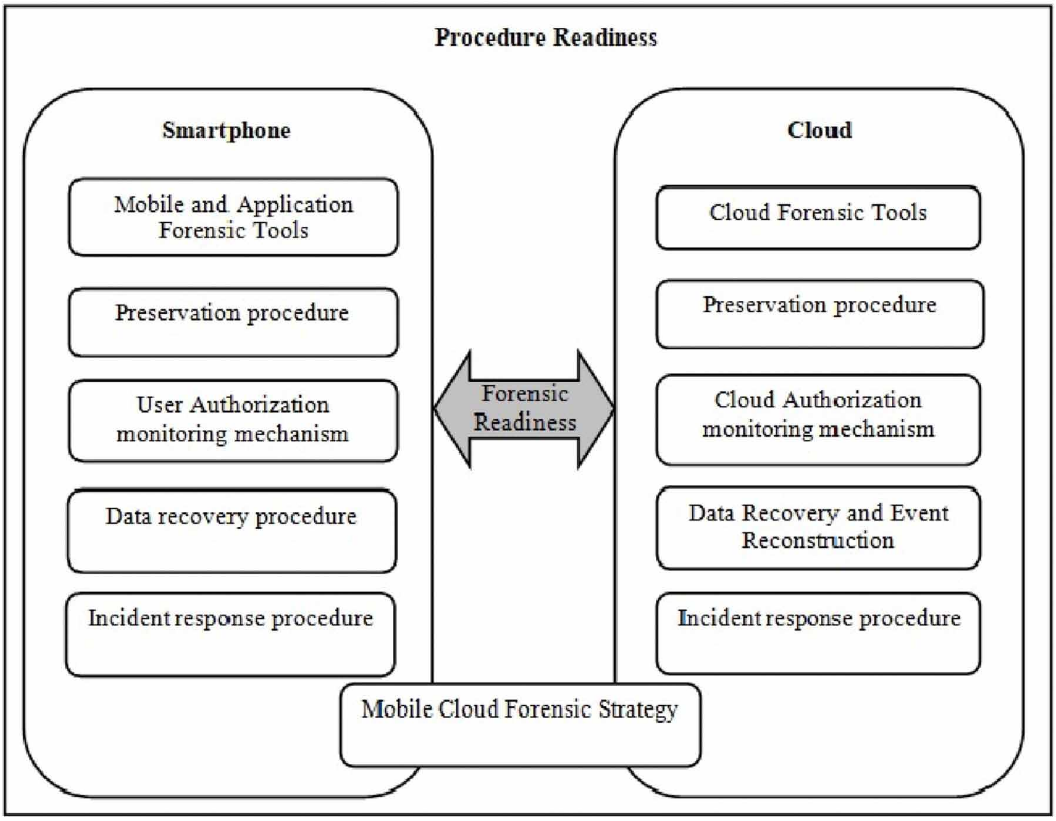
Figure 5. Sequence diagram for infrastructure readiness in mobile cloud forensics


Forensic Readiness Manager
Smartphone
Application Provider
Cloud
Cloud Service Provider
1. Acquire the user credentials
2. Enable the memory extraction
3. Exploit application interface
4. Request the access permission
5. Provide the access permission for communication logs
6. Enable data recovery mechanism
7.Request the SLA of the suspected user and request the access permission
8. Provide the data provenance and infrastructure transparency
9. Maintain long-term trust relationship
10. Enable logging and data fusion mechanism

between the physical machines. In the cloud environment, the guest OS deals with the challenges related to the timekeeping when executing the task either in a virtual or physical machine. In this scenario, the guest OS needs to initialize the clock at the right time and then, to update the time consistently. The sequential steps of the procedure readiness are depicted in Figure 7.

Forensic investigation is also associated with substantial and procedural legal requirements. In essence, the extracted evidence is to be relevant, reliable, authentic, and admissible based on the integrity of the investigation process as well as the integrity of the evidence itself. The judicial judgment is based on the evidence that belongs to a particular person committed an unlawful act at a specific time. To provide an admissible source of evidence for legal disputes, the law enforcement system performs the event reconstruction based on the sequence of investigation activities. Hence, applying

Figure 6. Procedure readiness in mobile cloud forensics


Procedure Readiness
Smartphone
Mobile and Application Forensic Tools
Preservation procedure
User Authorization monitoring mechanism
Data recovery procedure
Incident response procedure
Forensic Readiness
Cloud
Cloud Forensic Tools
Preservation procedure
Cloud Authorization monitoring mechanism
Data Recovery and Event Reconstruction
Incident response procedure
Mobile Cloud Forensic Strategy

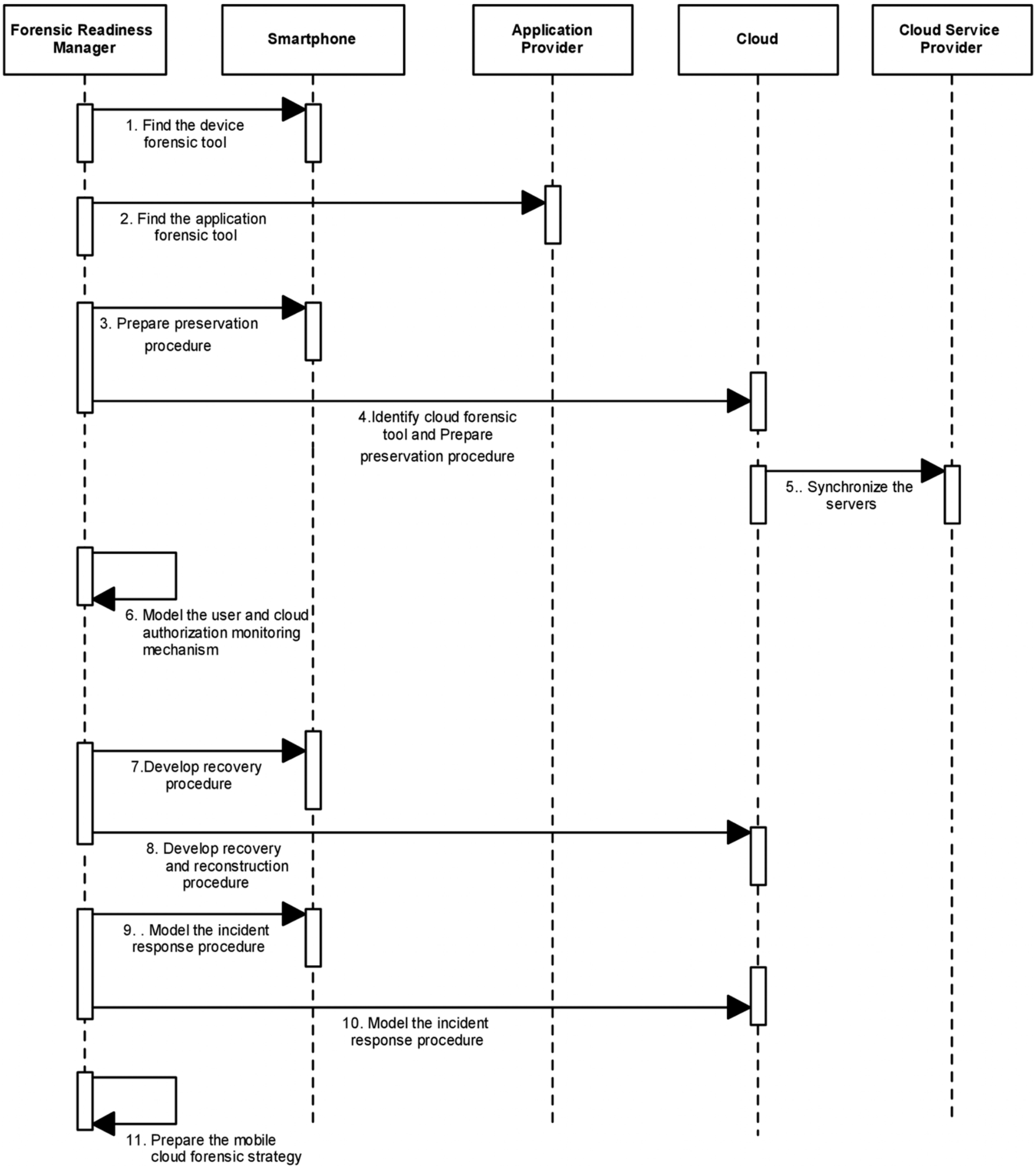
time synchronization becomes a non-trivial task in the forensic readiness to initiate the forensic investigation in both the mobile and cloud environments. As a result, time synchronization assists in improving the investigation, accuracy by mapping the mobile and cloud sequences of activities and also, to consistently validate the investigation by the law enforcement system.

4. TEST SCENARIO

This section demonstrates the proposed mobile cloud forensic readiness model for the cloud-based mobile application. The forensic readiness component supports an organization to provide the potential evidence to both the civil and criminal courts concerning the legal defense cases. It provides further benefits while conducting an investigation on a mobile cloud environment with legal proceedings, including cost minimization, improved interaction with law enforcement, incident impact evaluation. For instance, if an organization has involved in the civil litigation, the courts need the relevant data to the case for the legal proceedings. Hence, to produce digital evidence, many organizations develop the capability of forensic readiness to preserve the evidence consistently while performing the forensic investigation.

According to the standards of Digital Forensic Research Workshop (DFRWS) and National Security Agency (NSA), the proposed forensic readiness model supports the identification, preservation, collection, examination, analysis, presentation, and decision on the mobile cloud forensic investigation. In DFRWS, the four significant concerns need to be considered during the investigation, including a framework for digital forensic science, trustworthiness discussion of the

Figure 7. Sequence diagram for procedure readiness in mobile cloud forensics


Forensic Readiness Manager
Smartphone
Application Provider
Cloud
Cloud Service Provider
1. Find the device forensic tool
2. Find the application forensic tool
3. Prepare preservation procedure
4.Identify cloud forensic tool and Prepare preservation procedure
5.. Synchronize the servers
6. Model the user and cloud authorization monitoring mechanism
7.Develop recovery procedure
8. Develop recovery and reconstruction procedure
9. . Model the incident response procedure
10. Model the incident response procedure
11. Prepare the mobile cloud forensic strategy

evidence, hidden data detection, and recovery, and digital forensic science discussion in a networked environment. These considerations are taken into the account while modeling the proposed forensic readiness model for the mobile cloud forensics. With the support of NSA, the proposed forensic readiness model assures secure solutions to the identified vulnerabilities and follows the standards of NSA for the National Security System (NSS). Consequently, it preserves the privacy and security of the evidential information within NSS during the investigation.

The following steps describe the proposed forensic readiness model for the cloud-based mobile application forensics. For example, a test scenario discusses the proposed forensic readiness procedure for the existing forensic case study on the cloud-based mobile application (Farid, Dehghantanha, &

Choo, 2017). According to the case study, the test scenario demonstrates the forensic readiness model for the MEGA app on android device and cloud.

4.1. Step 1: Incident Recognition and Authorization

In the android smartphone, the proposed forensic readiness model performs incident monitoring and incident management. Consider, Incident monitoring module identifies that there is the occurrence of an intrusion in the MEGA app by monitoring the MEGA app storage database. In the incident management, the forensic readiness model prepares the encryption and hashing mechanism for the evidence acquired from the android device regarding the MEGA app. Also, it decides the decryption model for decrypting the files on the client devices due to the Advanced Encryption Standard (AES) algorithm based files encryption in the MEGA app. In the cloud, the forensic readiness model creates the path to acquire the cloud log files and analyze the evidence with the support of validation to store the evidence in the forensic database. Moreover, it creates the storage space for the corresponding incident in the evidence database and forensic readiness management database to manage the incident in the MEGA app.

4.2. Step 2: Infrastructure Readiness

In the android device, the proposed forensic readiness model also collects the information such as credentials, decryption mechanisms, and supported file types to facilitate the forensic activities of installation artifacts, login analysis, download analysis, and share analysis. Moreover, it prepares the internal storage, memory, and external storage of a Samsung Galaxy Tab II running Android Jelly Bean version 4.2 for evidence acquisition, and also, the API for the MEGA app. To perform the share, download, upload, and delete analysis, the forensic readiness model focuses on the communication logging with volatile data recovery permission. In the cloud, it requests permission for conducting the forensic investigation from the cloud service provider for the corresponding MEGA app related information access. Also, it decides that the mechanism for data fusion integrate the evidence of the MEGA app activities acquired from the various remote locations. In the mobile cloud environment, infrastructure readiness ensures that the potential evidence related to MEGA app activities to be readily available for further forensic investigation.

4.3. Step 3: Procedure Readiness and Time Synchronization

In the android device, the proposed forensic readiness model finalizes the required mobile and MEGA app forensic tools for the forensic identification phase. Moreover, it decides the incident response procedure, preservation procedure, authorization mechanism, and recovery procedure with the consideration of the incident, application category, file types, and so on. In the remote cloud, as similar to the android forensic procedure readiness model, the proposed forensic readiness model decides the procedures for the cloud forensics along with the selection of cloud forensic tools for acquiring the evidential artifacts of the MEGA app activities from the cloud server. Finally, the proposed mobile cloud forensic readiness model is responsible for deciding the mobile cloud forensic strategy with the time synchronization process for the corresponding incident.

In contrast to initiating the forensic investigation, such as login, upload, download, share, and delete analysis after beginning of the investigation request, the proposed forensic readiness model prepared the forensic environment with all the required factors before the investigation initiation and then, performs the investigation of the mobile cloud environment at the reduced time. Moreover, preliminary process of selecting the relevant information such as appropriate tools, procedures, mechanisms, and access permissions enforces the forensic investigation to the improved accuracy rather than extracting all the information from the mobile and cloud to decide the potential evidence at the time of the investigation. In subsequence, several potential readiness components involved in the proposed forensic readiness model improves the accuracy of the investigation from the inappropriate acquisition and analysis compared to the existing forensic readiness methods.

5. CONCLUSION

With the increasing popularity of mobile cloud computing, the numbers of threats to Smartphones, cloud, and cloud-based applications have also increased. Owing to the inherent characteristics of the mobile cloud, performing forensic investigation poses various challenges about evidence acquisition. An effective evidence acquisition or forensic preparation leads to the implementation of the consecutive forensic phases with minimum effort. This work developed an effective and efficient mobile cloud forensic readiness process model that proactively prepares the forensic environment to acquire a comprehensive set of potential evidence and investigate the crime event promptly. It also analyzes the mobile cloud environment and identifies the factors that influence the forensic readiness to facilitate the forensic investigation. The developed mobile cloud forensic readiness model observes the necessities of the forensic investigation and the characteristics of the potential evidence concerning a crime event to assist the forensic investigator. Thus, it significantly supports the forensic investigator to accomplish the improved investigation accuracy and the optimal investigation time while investigating the crime event about the cloud-based mobile applications.

REFERENCES

Ahmed, A., Zulkipli, N. H. N., Atlam, H. F., Walters, R. J., & Wills, G. B. (2017). The impact of cloud forensic readiness on seciruty. *International Conference on Cloud Computing and Services Science*, *2,* 539-545.

Alexios, M., Meletiadis, V., Tsoumas, B., Mitrou, L., & Gritzalis, D. (2012). Smartphone forensics: A proactive investigation scheme for evidence acquisition. *Proceedings of the IFIP International Information Security Conference (*pp. 249-260). Springer.

Aleksandar, V., & Venter, H. (2013). A harmonized process model for digital forensic investigation readiness. In *International Conference on Digital Forensics* (pp. 67-82). Springer.

Archit, G., Tyagi, A., & Agarwal, A. (2012). Smartphone forensic investigation process model *International Journal of Computer Science & Security*, *6*(5), 322–341.

Ben, M., Do, Q., & Choo, K.-K. R. (2015). Mobile cloud forensics: An analysis of seven popular Android apps.

Daryabar, F., Dehghantanha, A., & Choo, K.-K. R. (2017). Cloud storage forensics: MEGA as a case study. *The Australian Journal of Forensic Sciences*, *49*(3), 344–357.

Dilijonaite, A. (2017). Digital Forensic Readiness. In *Digital Forensics* (pp. 117–145). Wiley. doi:10.1002/9781119262442.ch4

George, S., Fogwill, T., Venter, H. S., & Ngobeni, S. (2013). *Digital forensic readiness in a cloud environment.* Proceedings of *IEEE AFRICON* (pp. 1–5). IEEE Press.

Grobler, C. P., Louwrens, C. P., & von Solms, S. H. (2010, February). A framework to guide the implementation of proactive digital forensics in organisations. *Proceedings of the 2010 International conference on availability, reliability and security* (pp. 677-682). IEEE.

Kamil, R., & Venter, H. S. (2013). The architecture of a digital forensic readiness management system. *Computers & Security*, *32*, 73–89. doi:10.1016/j.cose.2012.09.008

Kebande, V. R., Karie, N. M., & Omeleze, S. (2016). A Mobile Forensic Readiness Model aimed at Minimizing Cyber Bullying. *International Journal of Computers and Applications*, *140*(1).

Kebande, V. R., & Venter, H. S. (2014). A cloud forensic readiness model using a Botnet as a Service. *Proceedings of the International Conference on Digital Security and Forensics (DigitalSec2014)* (pp. 23-32). The Society of Digital Information and Wireless Communication.

Kebande, V. R., & Venter, H. S. (2017). Novel digital forensic readiness technique in the cloud environment. *The Australian Journal of Forensic Sciences*, 1–40.

Kebande Victor, R., & Venter, H. S. (2016). Requirements for achieving digital forensic readiness in the cloud environment using an NMB solution. *Proceedings of the 11th International Conference on Cyber Warfare and Security: ICCWS*. Academic Press.

Mohamed, E., Ahmad, A., Maynard, S. B., & Lonie, A. (2015). Digital forensic readiness: Expert perspectives on a theoretical framework. *Computers & Security*, *52*, 70–89. doi:10.1016/j.cose.2015.04.003

Mohamed, E., Maynard, S. B., Ahmad, A., & Lonie, A. (2014). Towards a systemic framework for digital forensic readiness. *Journal of Computer Information Systems*, *54*(3), 97–105. doi:10.1080/08874417.2014.11645708

Moses, D., Venter, H., Eloff, J., & Eloff, M. (2014). Requirements for preparing the cloud to become ready for digital forensic investigation. *Proceedings of the 13th European Conference on Cyber Warfare and Security ECCWS-2014*. Academic Press.

Moussa, A. N., Ithnin, N. B., & Miaikil, O. A. (2014, December). Conceptual forensic readiness framework for infrastructure as a service consumers. *Proceedings of the 2014 IEEE Conference on Systems, Process and Control (ICSPC 2014)* (pp. 162-167). IEEE.

Muhammad, F., Kechadi, T., & Le-Khac, N. A. (2015). The state-of-the-art forensic techniques in mobile cloud environment: A survey, challenges and current trends. *International Journal of Digital Crime and Forensics*, *7*(2), 1–19. doi:10.4018/ijdcf.2015040101

Muhammad, S., & Soomro, T. R. (2013). Impact of Smartphone's on Society. European journal of scientific research, 98(2), 216-226.

Percy, M. M., & Leonard, A. (2014). A conceptual framework to determine the digital forensic readiness of a Cloud Service Provider. *Proceedings of the IEEE Portland International Conference on Management of Engineering & Technology (PICMET)* (pp. 3313-3321). IEEE Press.

Pooe, A., & Labuschagne, L. (2012, August). A conceptual model for digital forensic readiness. *Proceedings of the 2012 Information Security for South Africa* (pp. 1-8). IEEE.

Rahman, A., Hidayah, N., Glisson, W. B., Yang, Y., & Choo, K.-K. R. (2016). Forensic-by-design framework for cyber-physical cloud systems. *IEEE Cloud Computing*, *3*(1), 50–59. doi:10.1109/MCC.2016.5

Raymond, C. K.-K. (2011). The cyber threat landscape: Challenges and future research directions. *Computers & Security*, *30*(8), 719–731. doi:10.1016/j.cose.2011.08.004

Serra, S. M., & Venter, H. S. (2011, August). Mobile cyber-bullying: A proposal for a pre-emptive approach to risk mitigation by employing digital forensic readiness. Proceedings of the 2011 Information Security for South Africa (pp. 1-5). IEEE. doi:10.1109/ISSA.2011.6027507

Shafique, Q. S., Ahmad, T., & Rafique, K. (2011). Mobile cloud computing as future for mobile applications-Implementation methods and challenging issues. *Proceedings of the IEEE International Conference on Cloud Computing and Intelligence Systems (CCIS)* (pp. 467-471). IEEE Press.

Soltan, A., Weber-Jahnke, J., & Traore, I. (2011). The proactive and reactive digital forensics investigation process: A systematic literature review. *Proceedings of the International Conference on Information Security and Assurance (*pp. 87-100). Springer.

Trenwith, P. M., & Venter, H. S. (2013). Digital forensic readiness in the cloud. In *Information Security for South Africa* (pp. 1–5). IEEE.

Valjarevic, A., & Venter, H. S. (2013, August). Implementation guidelines for a harmonised digital forensic investigation readiness process model. *Proceedings of the 2013 Information Security for South Africa* (pp. 1-9). IEEE.

Xian, Y., Jiang, L.-H., Shu, H., Yin, Q., & Liu, T.-M. (2009). A process model for forensic analysis of Symbian smart phones. *Proceedings of the International Conference on Advanced Software Engineering and Its Applications (*pp. 86-93). Springer.

Puneet Sharma received BE degree in Computer Science & Engineering from Annamalai University, Tamil Nadu, India, in 2011. He received his M.Tech degree in Computer Science & Engineering from SRM University, Tamil Nadu, India, in 2013. He is currently working as an Assistant Professor with the Department of Computer Science & Engineering, Amity University, Uttar Pradesh, India. Currently pursuing PhD from Amity University, Uttar Pradesh. His research and publication interest include mobile cloud computing techniques and mobile cloud forensic.

Deepak Arora is currently working as a Professor and Head of Department of Computer Science & Engineering, Amity University, Lucknow Campus. He has more than 15 years of teaching, research and industry experience. He received his PhD in Computer Science from Babasaheb Bhimrao Ambedkar University (A Central University), Lucknow in the year 2009. He has published more than 40 research publications to his credit in various Scopus, SCI, Thomson Reuters (Web of Science), ACM indexed international journals and more than 45 publications in Elsevier, Springer, ACM and IEEE international conferences. He has also supervised 3 PhDs.

T. Sakthivel received his Ph.D. in Information Technology and Computer Science Engineering from MS University, Tirunelveli, Tamilnadu, India in 2013. He has obtained B.E (CSE) from University of Madras and M. Tech (IT) from Punjabi University in 1995 and 2003 respectively. He has more than 20 years of experience in teaching, industry, and research. Currently, serving as a director at Firstsoft Technologies (P) Ltd, Chennai, and focusing on cutting-edge technologies and innovative products. His research interests mainly focus on wireless networks and security, digital forensics, mobile cloud computing, IOT, and machine learning. He is a professional member of the ACM.